looking .forward

The IEEE Computer Society's Student Newsletter

Summer 1997, Volume 5, No. 2

This issue edited by IEEE Computer Society Student Chapter of Virginia Tech, Blacksburg, VA

Table of Contents

A Short Tutorial on Wireless LANs and IEEE 802.11

Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman

The Bradley Department of Electrical and Computer Engineering

Virginia Polytechnic Institute and State University

Blacksburg, Virginia 24061-0111

dlough@vt.edu, blanken@vt.edu, kkrizman@vt.edu

---

1. Introduction

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the face of the earth. Hundreds of millions of people exchange information every day using pagers, cellular telephones, and other wireless communication products. With tremendous success of wireless telephony and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere they venture. This article will try to answer some basic questions of why and where wireless local area networks can be used, and present a brief description of some protocols that have been developed, with emphasis on IEEE 802.11.

2. Some Motivation

Since the success of the Ethernet project at Xerox's Palo Alto Research Center in the early 1970's [1] and other similar digital protocols, the basic technology has been in place for local area networks (LANs) to blossom in both the public and private sectors. Standard LAN protocols, such as Ethernet, that operate at fairly high speeds with inexpensive connection hardware can bring digital networking to almost any computer. Today, organizations of every size access and share information over a digital network; the power of networking and collaborative, distributed computing is beginning to be realized. However, until recently, LANs were limited to the physical, hard-wired infrastructure of the building. Even with phone dial-ups, network nodes were limited to access through wired, land line connections. Many network users, especially mobile users in businesses, the medical profession, factories, and universities, to name a few, find benefit from the added capabilities of wireless LANs [2]

The major motivation and benefit from wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere. Examples of the practical uses for wireless network access are limited only by the imagination of the application designer. Medical professionals can obtain not only

patient records, but real-time vital signs and other reference data at the patient bedside without relying on reams of paper charts and physical paper handling. Factory floor workers can access part and process specifications without impractical or impossible wired network connections. Wireless connections with real-time sensing allows a remote engineer to diagnose and maintain the health and welfare of manufacturing equipment, even on an environmentally-hostile factory floor. Warehouse inventories can be carried out and verified quickly and effectively with wireless scanners connected to the main inventory database. Even wireless "smart" price tags, complete with liquid crystal display (LCD) readouts, allow merchants to virtually eliminate discrepancies between stock-point pricing and scanned prices at the checkout lane. The list of possibilities is almost endless.

In addition to increased mobility, wireless LANs offer increased flexibility. Again, imagination is the limiting parameter. One can visualize without too much difficulty a meeting in which employees use small computers and wireless links to share and discuss future design plans and products. This "ad hoc" network can be brought up and torn down in a very short time as needed, either around the conference table and/or around the world. Some car rental establishments already use wireless networks to help facilitate check-ins. Traders on Wall Street are able to use wireless terminals to make market trades. Even students of university campuses have been known to access lecture notes and other course materials while wandering about campus.

Sometimes it is more economical to use a wireless LAN. For instance, in old buildings, the cost of asbestos cleanup or removal outweighs the cost of installing a wireless LAN solution. In other situations, such as a factory floor, it may not be feasible to run a traditional wired LAN. Wireless LANs offer the connectivity and the convenience of wired LANs without the need for expensive wiring or rewiring.

3. Mobile IP

Mobile IP [3] was suggested as a means to attain wireless networking. It focuses its attention at the Network Layer, working with the current version of the Internet Protocol (IP version 4). In this protocol, the IP address of the mobile machine does not change when it moves from a home network to a foreign network. In order to maintain connections between the mobile node and the rest of the network, a forwarding routine is implemented.

When a person in the physical world moves, they let their home post office know to which remote post office their mail should be forwarded. When the person arrives at their new residence, they register with the new post office. This same operation happens in Mobile IP. When the mobile agent moves from its home network to a foreign (visited) network, the mobile agent tells a home agent on the home network to which foreign agent their packets should be forwarded. In addition, the mobile agent registers itself with that foreign agent on the foreign network. Thus, all packets intended for the mobile agent are forwarded by the home agent to the foreign agent which sends them to the mobile agent on the foreign network. When the mobile agent returns to its original network, it informs both agents (home and foreign) that the original configuration has been restored. No one on the outside networks need to know that the mobile agent moved.

This configuration works, but it has some drawbacks. Depending on how far the mobile agent moves, there may need to be some store and forwarding of packets while the mobile agent is on neither the home nor the foreign network. In addition, Mobile IP works only for IPv4 and does not take advantage of the features of the newer IPv6.

4. IEEE 802.11 Architectures

In IEEE's proposed standard ~~for wireless~~ LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network ~~"on the fly."~~ As shown in Figure 1, there is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. A good example of this is the aforementioned meeting where employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) [4] have been designed to "elect" one machine as the base station (master) of the network with the others being slaves. Another algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.

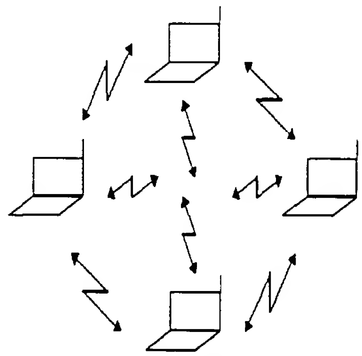

Figure 1: Ad-Hoc Network

As shown in Figure 2, the second type of network structure used in wireless LANs is the infrastructure. This architecture uses fixed network access points with which mobile nodes can communicate. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular networks around the world.

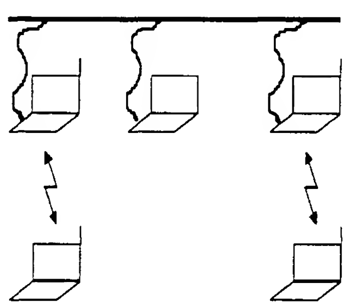

Figure 2: Infrastructure Network

5. IEEE 802.11 Layers

The IEEE 802.11 standard places specifications on the parameters of both the physical (PHY) and medium access control (MAC) layers of the network. The PHY layer, which actually handles the

transmission of data between nodes, can use either direct sequence spread spectrum, frequency-hopping spread spectrum, or infrared (IR) pulse position modulation. IEEE 802.11 makes provisions for data rates of either 1 Mbps or 2 Mbps, and calls for operation in the 2.4 - 2.4835 GHz frequency band (in the case of spread-spectrum transmission), which is an unlicensed band for industrial, scientific, and medical (ISM) applications, and 300 - 428,000 GHz for IR transmission. Infrared is generally considered to be more secure to eavesdropping, because IR transmissions require absolute line-of-sight links (no transmission is possible outside any simply connected space or around corners), as opposed to radio frequency transmissions, which can penetrate walls and be intercepted by third parties unknowingly. However, infrared transmissions can be adversely affected by sunlight [5], and the spread-spectrum protocol of 802.11 does provide some rudimentary security for typical data transfers.

The MAC layer is a set of protocols which is responsible for maintaining order in the use of a shared medium. The 802.11 standard specifies a carrier sense multiple access with collision avoidance (CSMA/CA) protocol. In this protocol, when a node receives a packet to be transmitted, it first listens to ensure no other node is transmitting. If the channel is clear, it then transmits the packet. Otherwise, it chooses a random "backoff factor" which determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in which the channel is clear, the transmitting node decrements its backoff counter. (When the channel is busy it does not decrement its backoff counter.) When the backoff counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same backoff factor is small, collisions between packets are minimized. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11. The reason for this is that when a node is transmitting it cannot hear any other node in the system which may be transmitting, since its own signal will drown out any others arriving at the node.

Whenever a packet is to be transmitted, the transmitting node first sends out a short ready-to-send (RTS) packet containing information on the length of the packet. If the receiving node hears the RTS, it responds with a short clear-to-send (CTS) packet. After this exchange, the transmitting node sends its packet. When the packet is received successfully, as determined by a cyclic redundancy check (CRC), the receiving node transmits an acknowledgment (ACK) packet. This back-and-forth exchange is necessary to avoid the "hidden node" problem, illustrated in Figure 3. As shown, node A can communicate with node B, and node B can communicate with node C. However, node A cannot communicate node C. Thus, for instance, although node A may sense the channel to be clear, node C may in fact be transmitting to node B. The protocol described above alerts node A that node B is busy, and hence it must wait before transmitting its packet.

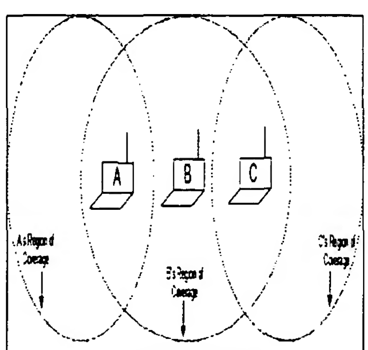

Figure 3: The hidden node problem

6. Conclusions

IEEE 802.11 is still in the process of being adopted as a standard by the IEEE standards body. Although 802.11 provides a reliable means of wireless data transfer, some improvements to it have been proposed. For example, at Virginia Tech, research is being performed into ways in which the 802.11 network parameters can be dynamically adjusted to improve throughput [6] [7]. The use of wireless LANs is expected to increase dramatically in the future as businesses discover the enhanced productivity and the increased mobility that wireless communications can provide in a society that is moving towards more connectionless connections.

7. References

[1] R.M. Metcalfe and D.R. Boggs, "Ethernet: Distributed Packet Switching for Local Computer Networks," Communications of the Association for Computing Machinery, Vol. 19, pp. 395-404, July 1976.

[2] L. Goldberg, "Wireless LANs: Mobile Computing's Second Wave," Electronic Design, 26 June 1995.

[3] C. Perkins, "IP Mobility Support," RFC 2002, October 1996.

[4] K. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September / October 1994.

[5] T.S. Rappaport, private communication, June 1997.

[6] B.E. Mullins, N.J. Davis IV, and S.F. Midkiff, "A Wireless Local Area Network Protocol That Improves Throughput Via Adaptive Control," Proceedings of the IEEE International Conference on Communications, pp. 1427-1431, June 1997.

[7] B.E. Mullins, N.J. Davis IV, and S.F. Midkiff, "An Adaptive Wireless Local Area Network Protocol That Improves Throughput Via Adaptive Control of Direct Sequence Spread Spectrum Parameters, to appear in ACM Mobile Computing and Communication Review, Vol. 1, No. 3, 1997.

Back to Table of Contents